

**REMARKS**

The Examiner is thanked for the thorough examination of the present application.

The FINAL Office Action, however, has tentatively rejected all claims 1-36. Claims 1-3 and 5-13 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Yamada et al. (U.S. Pat. No. 6,490,683, hereinafter “Yamada”) in view of Ohgake (U.S. Pub. No. 2001/0044887). Claims 14-28 and 30 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Yamada, in view of Ohgake, further in view of Ando et al. (U.S. Pat. No. 6,907,187, hereinafter “Ando”). Claim 4 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Yamada, in view of Ohgake, further in view of Sasaki et al. (U.S. Pub. No. 2002/0051630, hereinafter Sasaki). Claims 31-36 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Yamada, in view of Ohgake, further in view of Serpa (U.S. Pat. No. 6,954,862). Claim 29 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Yamada, in view of Ohgake, further in view of Ando, further in view of Serpa (U.S. Pat. No. 6,954,862).

In response, Applicant submits the foregoing amendments and following remarks. In this response claims 1 and 31 have been amended, and claims 3 and 4 have been canceled. Applicant respectfully requests consideration of the following remarks contained herein. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

**Response to Claim Rejections Under 35 U.S.C. § 103**

The FINAL Office Action has tentatively rejected claims 1-36. For at least the reasons set forth below, Applicant traverses these rejections.

### **Independent Claim 1**

Applicants respectfully submit that independent claim 1 patentably defines over Yamada, in view of Ohgake for at least the reason that the combination fails to disclose, teach or suggest the features emphasized below in claim 1.

Claim 1, as amended, recites (emphasis added):

1. A method for encoding a confidential optical disc with a burner, the method comprising the steps of:
  - receiving signal of creating confidential optical disc to switch burner into a burning mode;
  - setting a data-accessing password for future verification, **wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc;**
  - selecting one of data sources for public viewing and confidential viewing data to be burned on the disc;
  - receiving a start burn signal to begin data encoding process;
  - creating a temporary file system as buffer that includes two stages, creating standard file set and creating parallel file set with real data; and
  - burning buffer to an optical disc and produce a tangible disc.

Applicant has amended claim 1 to further define certain aspects of the claimed embodiment in claim 1. Claims 3 and 4 have been canceled. Applicant submits that no new matter is added by the amendment. As indicated above, claim 1 now recites the element, “wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc.” Applicant submits that neither Yamada nor Ohgake teach this feature.

The secret file set descriptor (see, e.g., component 310, in Fig. 3) in claim 1 is pointed by the address stored in the sequence (302) and can only be found by the specified optical disc player/reader. Moreover, in order to maintain confidentiality of the disc, two different sets of data are defined on the optical disc – dummy data and real

data. (Claim 1 recites: “creating a temporary file system as buffer that includes two stages, creating standard file set and creating parallel file set with real data”). For this embodiment, a conventional optical disc reader/player can only read the dummy data and in contrast, the real data can only be found and read by specified optical disc reader/players. Furthermore, according to the confidential optical disc encoding process described in Fig. 4 in the specification of the claimed invention, the burner will switch to a confidential disc burning mode and promptly request a data-accessing password.

In the **Response to Arguments** section, the Office Action maintains that the Yamada reference teaches the feature, “setting a data-accessing password for future verification.” Claim 1, as amended, now recites “setting a data-accessing password for future verification, *wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc.*” Applicant respectfully submits that Yamada fails to teach this feature. Applicant refers to the text passage cited in the Office Action (emphasis added):

Thus, data having a copy protecting password (being electronic watermark data formed in the electronic watermark pattern forming process S119) formed in the ECC block forming process S116 that needs to be protected from dishonest copying is recorded on the data recording medium (such as a DVD-RAM disk) 201 in step (S121).  
(Col. 19, lines 41-46).

When reproducing data from the data recording medium, both the user password in the file identifier descriptor FID and the password in the electronic watermark data are read out and compared to each other. This process determines whether a third party has renewed the file data.  
(Col. 19, line 66 to Col. 20, line 2).

While Yamada teaches of a “copy protecting password,” nowhere does Yamada teach,

“wherein the data-accessing password is placed to a secret file set descriptor and allocated on any unoccupied space of an optical disc.” At most, Yamada teaches of a user password in the file identifier descriptor (FID). However, Applicant respectfully submits that the “user password” disclosed by Yamada is not equivalent to the “data-accessing password” recited in claim 1. For the claimed embodiment in claim 1, the data-accessing password can be found via a password address containing the secret file set descriptor.

Even assuming, *arguendo*, that the user password taught by Yamada is equivalent to the data-accessing password in claim 1 (as the Examiner maintains in the **Response to Arguments** section), Yamada nevertheless fails to teach the element, “wherein the data-accessing password is . . . allocated on any unoccupied space of an optical disc.” A specified ID field and the data-accessing password can be stored in a specified area (e.g., implementation user volume descriptor). However, they can also be allocated anywhere on an optical disc, as long as the storing space does not have a piece of data or descriptor’s address fixed by a file system or an application layer. Applicant respectfully submits that the Yamada reference fails to teach this feature. Furthermore, the Ohgake reference fails to address this deficiency.

Accordingly, Applicant respectfully submits that independent claim 1 patently defines over Yamada in view of Ohgake for at least the reason that the combination fails to disclose, teach or suggest the highlighted features in claim 1 above.

### **Claim 31**

Applicants respectfully submit that claim 31 patently defines over Yamada, in view of Ohgake, further in view of Serpa for at least the reason that the combination fails to disclose, teach or suggest the features emphasized below in claim 31.

Claim 31, as amended, recites (emphasis added):

31. A method for reading a confidential optical disc, which is a decoding method for reading optical disc produced by claim 1, the method comprising steps of:

player reading optical disc data;  
receiving view confidential data command signal;  
**requesting entry of a data-accessing password;**  
checking to determine if password entries reach a predetermined limitation;

if password entries do not reach the predetermined limitation, checking if correct ID field exist;

**if ID field exists in the optical disk, checking if entered password is correct;**

**if entered password is correct, playing/reading real data;**  
and  
ending playing/reading session.

Applicant has amended claim 31 to clarify certain aspects of the claimed

embodiment in claim 31. Applicant submits that no new matter is added by the amendment. As indicated above, claim 31 now recites the element, “requesting entry of **a data-accessing password.**” Applicant submits that none of the cited references (*i.e.*, Yamada, Ohgake, and Serpa) teaches this feature. In particular, none of the references disclose, teach, or suggest “a data-accessing password.”

On page 15, the Office Action relies on the Ohgake reference to allegedly teach this feature (“*requesting to entry of a password* [*[(lines 3-8 of [0038] from Ohgake*”). The relevant portion of paragraph 38 from Ohgake is reproduced below (emphasis added):

[0038] On the other hand, if it is determined at the step S1 that the optical disk 1 includes the record-medium identification information “d”, the record-medium accessing software 12 determines that the optical disk 1 is the peculiar optical disk 1.sub.new according to the present invention, and proceeds to a step S2. At the step S2,

the record-medium accessing software 12 requests a user to input qualification information such as a password, . . .

(Par. 38). While Ohgake teaches that the record-medium accessing software requests from the user qualification information (such as a password), Applicant submits that this qualification information is not equivalent to the “data-accessing password” recited in claim 31. Indeed, Ohgake teaches of “comparing the qualification information inputted by the user and pre-registered qualification” to determine whether the qualification of the user is correct. (See Ohgake, Par. 39.) As such, Applicant submits that Ohgake fails to teach this feature. Furthermore, the cited Yamada and Serpa references fail to address this deficiency.

Finally, Applicant respectfully maintains that nowhere do the cited references disclose or suggest playing/reading real data if entered password is correct. Claim 31 recites: “if ID field exists in the optical disk, checking if entered password is correct” and “if entered password is correct, playing/reading real data.” The cited references fail to teach this element.

Accordingly, Applicant respectfully submits that claim 31 patently defines over Yamada, in view of Ohgake, further in view of Serpa for at least the reason that the combination fails to disclose, teach or suggest the highlighted features in claim 31 above.

### **Dependent Claims 2, 5-30, and 32-36**

Applicants submit that dependent claims 2, 5-30, and 32-36 are allowable for at least the reason that these claims depend from an allowable independent claim. See, e.g., *In re Fine*, 837 F. 2d 1071 (Fed. Cir. 1988).

## **CONCLUSION**

Applicant respectfully submits that all pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephone conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

No fee is believed to be due in connection with this amendment and response to Office Action. If, however, any fee is believed to be due, you are hereby authorized to charge any such fee to deposit account No. 20-0778.

Respectfully submitted,

/Daniel R. McClure/

---

**Daniel R. McClure  
Reg. No. 38,962**

**THOMAS, KAYDEN, HORSTEMEYER  
& RISLEY, L.L.P.**  
100 Galleria Parkway NW  
Suite 1750  
Atlanta, Georgia 30339  
(770) 933-9500